ネットコケーション研究部門活動報告

武藏 泰雄† 久保田 真一郎† 杉谷 賢一†

†熊本大学総合情報基盤センター・ネットコミュニケーション研究部

概要: 2002 年の発足以来当研究部門は、DNS サーバの名前解決要求パケット通信のログを収集し、学内の様々なセキュリティインシデントやネットワーク障害事案と照合することによって、学内ネットワーク(KUIC)の安全安心な利用のために必要な知見を得て来た。今回は DNS サーバまたは DNS サービスそのもの、あるいは大学のネットワークに対するサービス妨害活動を思われる事案、すなわち DNS ANY Request Cannon (DARC)活動事案について報告する。

1. 背景

2002 年 4 月に総合情報基盤センターが発足して以来、ネットワーク研究部では、将来実施されると予測される大学のネットワークに対するサイバー攻撃事案に対応するため、Domain Name System (DNS) サーバや E-mail サーバ、または Web サーバ等、様々なネットワークサーバのシステムログの解析を行っている。特に DNS サーバの名前解決要求パケット通信ログに関する解析結果は、学内ネットワークにおける様々なセキュリティ事案や障害事案と照合することによって、セキュリティ事案やインシデントの被害緩和や未然に対応するための知見を与えることが判明しているため、有用な情報を与える。

今回は、DARC (DNS ANY Request Cannon)活動[1,2]というサイバーセキュリティ事案について検討したので報告したい。この DARC 活動は、平成 23 年 11 月 28 日から本学の情報ネットワークにおいても観測され始めた(図 1)。その活動内容は、単にドメイン名"kumamoto-u.ac.jp"についての名前解決(リソースレコードは ANY 型)を活動期間中に繰り返すだけである。平成 24 年から本格的検討に入り、その検討結果は、平成 25 年 11 月 1 日に中国瀋陽開催された国際学会 IEEE ICINIS2013 で発表された[3]。また国際学会のジャーナルにも 2014 年 3 月に掲載された(平成 25 年 7 月 15 日以降は観測されていない)[4,5]。

2. DARC 活動の検知システムの開発とその評価

DARC 活動は、単一ドメイン名(kumamoto-u.ac.jp)の名前解決要求を送信対象の DNS サーバに対して繰り返すだけの活動である。これを DARC 活動の定義とする。具体的には、DNS サーバに対して ANY リソースレコード(RR)型 DNS クエリ要求パケットを送信することで実現される。DNS クエリのログデータから 1 日当たりのデータセットを作成し、ログメッセージ単位に含まれる DNS クエリキーワード間の編集距離を計算し、その距離が 0 であることを利用すれば、DARC 活動は検知できる。リアルタイム性を確保するため、現在のドメイン名 X(=FQDN$_i$)と直前のパケットの各々のドメイン名 Y(=FQDN$_{i-1}$)について Levenshtein 編集距離 LD(X,Y)を求める[6,7]。

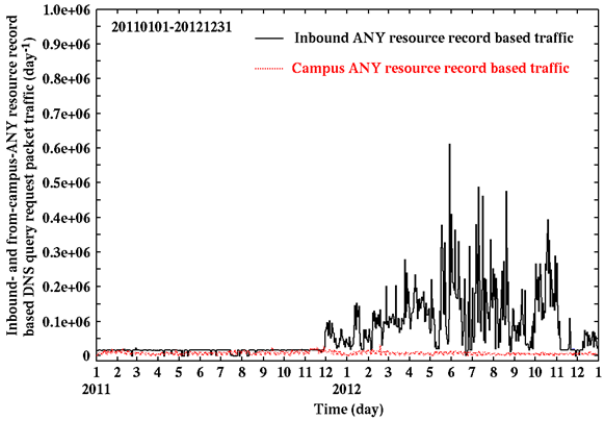

図 1. ANY リソースレコード型 DNS クエリ要求パケット通信流量の変化(実線は学外からの通信流量、点線は学内からの通信流量:単位は day^{-1})

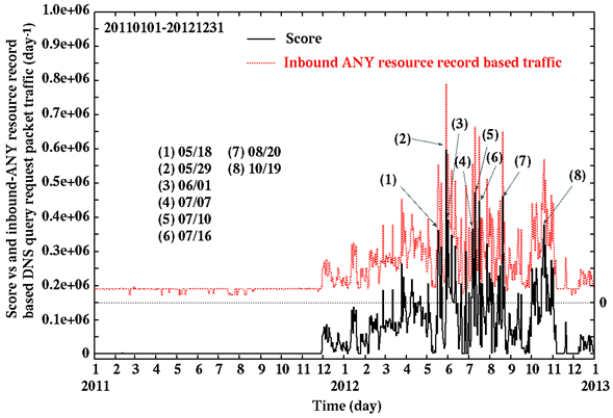

図 2. 検知スコアの変化と学外からの ANY リソースレコード型 DNS クエリ要求パケット通信流量の変化(実線はスコアの変化量、点線は学外からの通信流量:単位は day^{-1})

$$LD[x,y] = \min(LD[x-1][y]+1, LD[x][y-1]+1, LD[x-1][y-1]+\text{cost}) \quad (1)$$

式 1 における x と y は文字列 X と Y の長さである。DARC の定義から検知条件は、編集距離 LD(X, Y)= LD(FQDN$_i$, FQDN$_{i-1}$)=0 である。

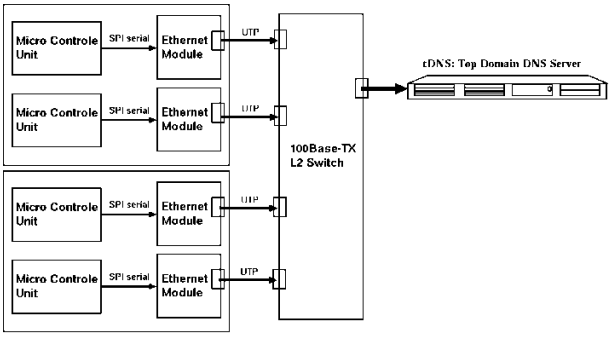

図 3. DNS クエリ要求パケットトラフィック生成器

検知された DNS クエリパケット数を積算してスコアを計算し、図 2 に 2011 年 1 月 1 日-2012 年 12 月 31 日の期間の検知結果を示した。

図 2 における、実戦と点線は良く似ているところから、学外からの ANY RR 型 DNS クエリ要求パケット通信流量のほとんど DARC 活動によるものと考えられる。

3. DARC 活動装置の開発とサーバに対する負荷測定結果

ところでこの DARC 活動[1,2]は何のために実施される理由について考察を試みる。

通常 DNS サーバが ANY RR 型 DNS クエリ要求パケットを受信すると、応答可能なすべての登録情報を DNS クエリ応答パケットに詰め込んで送信元 IP アドレスへ送り返す。仮に DNS サーバが DNSSEC を導入して応答パケットが大きくなっている場合、名前解決繰り返えす場合（例えば isc.org 等は 3KB の応答パケット返す）、DNS サーバへ大きな負荷が掛かる。そのため DNS サーバは DoS 攻撃を受ける。検討当初では、DARC 活動同様の活動ではないかと考えられた。しかし本大学が応答する最大のサイズは、226B でありそれほど大きな負荷が掛からないと考えられる。また以前平成 22 年度の当センター広報でも報告した通りクエリキーワードが単一であるところから Kaminsky 型の攻撃ではない（Kaminsky 型ではユニークなクエリキーワードを大量に送り付ける）[8]。これらの理由により、本大学の DNS サーバに対して DARC 活動を実施する理由が現時点では不明である。

しかしながら、念のため DARC 活動によってどれくらいの負荷が DNS サーバへ掛かるのかを調査する必要がある。

そこで、DARC 活動を再現する DQRPTGS (DNS Query Packet Traffic Generating System: 図 3)を開発した。この装置は 4 個の 8bit Micro Controller Unit (MCU: ATmega328P-PU)[9]、4 個の SPI 制御型 Ethernet Module(WIZnet WIZ820io)[10]、および 100Base-TX の L2 switching HU(L2-SW)B から構成されている。この装置は、MCU と Ethernet Module を使用して DNS クエリ要求パケットを毎秒 62-63 クエリ生成可能で、更に

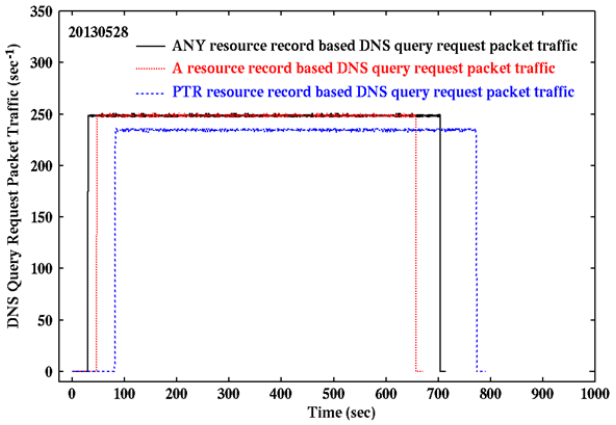

図 4. 生成された DNS クエリ要求トラフィック（ANY, A, and PTR）

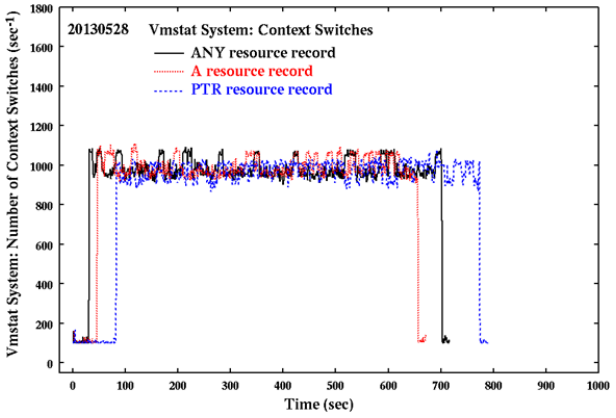

図 4. 生成された DNS クエリ要求トラフィック（ANY, A, and PTR）

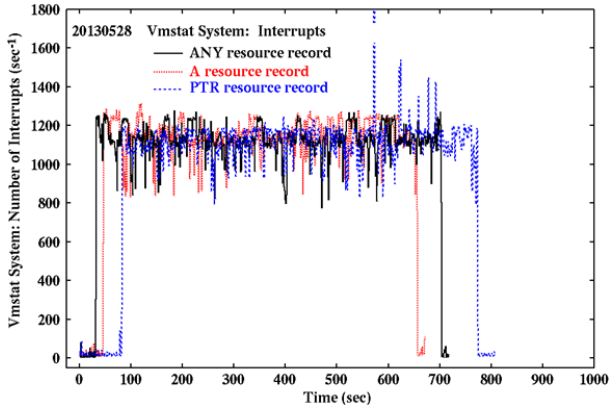

図 4. 生成された DNS クエリ要求トラフィック（ANY, A, and PTR）

L2-SW で集約して、毎秒 250 クエリの負荷を DNS サーバに掛けることが可能である。生成されるクエリキーワードは DNS サーバのキャッシュをさけるためユニークになるように設定されている。

図 4 に DQRPTGS で ANY RR、A RR、PTR RR の DNS クエリ要求パケットトラフィックを発生させ、実験用 DNS サーバに対する負荷テストを行った。負荷の測定は、DNS サーバ上の vmstat を使用した。測定パラメータとして Context Switch と Interrupts を選択し、その結果を図 5 と 6 に示す。

図 5 において、ANY RR、A RR および PTR RR それぞれの CS はほぼ同じ値で、同様の分布を示している。また図 6 における Interrupts についても良く似た結果である。すなわち ANY RR でも A RR でも DNS サーバに対する負荷は大差がないこと示している。

5. まとめ

2013 年度に本研究部門で行った研究成果を報告した。2011 年 11 月 28 日から続いていた DARC 活動は 2013 年 7 月 15 日で中止された。この活動が DoS 攻撃の一環であるかどうかは現在も不明である。また、DARC 活動に関する研究より、DNS サーバへの負荷とは何かというのを定義する良い機会となった。今後の研究課題として、サーバの負荷を測定する技術を確立したい。以上の研究成果は中国瀋陽開催された国際学会 IEEE ICINIS2013 で発表された。また国際学会のジャーナルにも 2014 年 3 月に掲載された

謝辞

我々の研究はすべて総合情報基盤センターの設備を使って行われた。熊本大学の教職員及び学生の皆様のご理解ご協力に心より感謝したい。

参考文献

[1] T. Daly, “Observed DNS Anomaly: Bumps in DNS ANY Query Activity,” *Dyn Inc*., Manchester, NH, 2011,http://www.dyncommunity.com/questions/22190/observed-dns-anomaly-bumps-in-dns-any-query-activi.html

[2] K. Shortt, “DNS ANY Request Cannon - Need More Packets”, *Internet Storm Center (ISC) Diary*, SANS Technology Institute 2012, https://isc.sans.edu/diary.html?date=2012-05-21

[3] Yuto Takeda, Yasuo Musashi, Keinchi Sugitani, and Toshiyuki Moriyama, "DNS ANY Request Cannon Activity in DNS Query Request Packet Traffic," Proceedings of the Sixth International Conference on Intelligent Networks and Intelligent Systems (ICINIS 2013), Shenyang, China, pp. 181-184 (2013)

[4] Yasuo Musashi, Yuto Takeda, Nobuhiro Shibata, Shinichiro Kubota, and Keinchi Sugitani, "A Statistical Study of ANY Resource Record Based DNS Query Request Packet Traffic," Information, Vol. 16, No. 12(B), pp. 8901-8908 (2013)

[5] Yuto Takeda, Yasuo Musashi, Keinchi Sugitani, and Toshiyuki Moriyama, "DNS ANY Request Cannon Activity in DNS Query Packet Traffic," International Journal of Intelligent Engineering and Systems Vol. 7 , No. 1, pp. 8-16 (2014)

[6] V. L. Levenshtein, “Binary codes capable of correcting deletions, insertions, and reversals”, Soviet Physics Doklady, Vol. 10, No. 8, pp.707-710, 1966.

[7] F. J. Damerau, “A technique for computer detection and correction of spelling errors”, Communications of the ACM, Vol. 7, No. 3, pp.171-176 (1964).

[8] D. Kaminsky: It’s The End of The Cache As We Know it,” 2008, http://kurser.lobner.dk/dDist/DMK_BO2K8.pdf.

[9] Atmel AVR Atmega328P-PU: http://www.atmel.com/devices/ATMEGA328P.aspx

[10] Wiznet W5100/W5200 Ethernet chip: http://www.wiznet.co.kr/UpLoad_Files/ReferenceFiles/W5200_DSV129E.pdf